Oracle® E-Business Suite Concepts

High Availability

Introduction

The subject of High Availability covers a range of standard features and additional options that help to minimize planned and unplanned downtime, or facilitate recovery after a period of downtime. They include:

- Patching Hints and Tips
- Shared Application Tier File System
- Distributed AD
- Nologging Operations
- Disaster Recovery

This section will provide a high-level guide to the key features that can help make an Oracle E-Business Suite highly available, with the emphasis on guidelines for making the correct decisions when planning a new installation or upgrade.

Note: High availability is greatly facilitated by the *online patching* capability introduced in Oracle E-Business Suite Release 12.2. This key feature is described in Chapter 5.

High Availability Principles

In addition to taking full advantage of online patching, other strategies for high availability include:

- **Keep AD up-to-date** - Running at the latest AD mini-pack level allows you to take full advantage of new features designed to reduce downtime and simplify maintenance.
- **Apply the latest software updates** - The more up-to-date your system, the less likely you are to experience known problems, and the easier it will be to resolve any new issues that may arise.
- **Consolidate multiple patches** - Merging multiple Oracle E-Business Suite patches into a single patch minimizes the scope for error that would arise in applying a number of separate patches. This can now be undertaken by the adop utility, although the traditional AD Merge Patch utility is still available for use in specialized cases.
- **Keep your test system current with your production system** - When you test the application of a patch, the test must be realistic in terms of current patch level and transaction data: you can employ either Oracle Applications Manager or the Rapid Clone tool to create a copy of your production system for tests.

Where applicable, these strategies are described further below.

Note: For full details of carrying out patching and maintenance operations, see the Patching and Managment Tools chapter of this book, and the relevant chapters of *Oracle E-Business Suite Maintenance Guide*.

Disaster Recovery

A significant problem that strikes an Oracle E-Business Suite installation could put the viability of the organization at risk. Such a problem could be:

- An external disaster, such as a fire at a company's data center, resulting in a loss of service that severely hampers the organization's ability to do business.
- An internal disaster, such as a serious error by a privileged user, resulting in major loss or corruption of data.
- A hardware or system failure or malfunction, such as a media failure, or operating system problem that corrupts the actual data in the database

This section gives an overview of the area of disaster recovery, which can be considered as the final component of a high availability strategy. Disaster recovery involves taking steps to protect the database and its environment to ensure that they can still operate in the face of major problems. Oracle provides features such as *Oracle Data Guard* and *Flashback Database* .

- Data Guard is used to set up and maintain a secondary copy of a database, typically referred to as a *standby database*. Such a standby database is brought into use after a *failover* from the primary database when the primary becomes unavailable following a significant problem, or via a switchover operation that is executed to allow service to continue during planned maintenance of the environment's platform or building services.
- Flashback Database is used to "rewind" a database to a prior point in time, making it possible to recover from major logical corruptions of a database without requiring a complete restore.

You must also install any other hardware and software required to run your standby environment as a production environment after a failover, ensuring that any changes on the primary are matched on the standby. Examples include tape backup equipment and software, system management and monitoring software, and other applications.

Oracle Data Guard and Oracle E-Business Suite Release 12.2

Oracle Data Guard provides mechanisms for propagating changes from one database to another, to avoid possible loss of data if one site fails. The two main variants of a Data Guard configuration are *Redo Apply* (often referred to as *Physical Standby*) and *SQL Apply* (often referred to as *Logical Standby*). . Both of these use the primary database's redo information to propagate changes to the standby database.

- Physical standby uses the normal database recovery mechanism to apply the primary database's redo to the standby database, resulting in an identical copy of the production database.
- Logical standby employs the Oracle LogMiner utility to build SQL statements that recreate changes made to the data. The logical standby mechanism is not currently utilized with Oracle E-Business Suite.

The secondary environment should be physically separate from the primary environment, to protect against disasters that affect the entire primary site. This necessitates having a reliable network connection between the two data centers, with sufficient bandwidth (capacity) for peak redo traffic. The other requirement is that the servers at the secondary site are the same type as at the primary site, in sufficient numbers to provide the required level of service; depending on your organization's needs, this could either be a minimal level of service (supporting fewer users), or exactly the same level of service as you normally provide.

Data Guard's reliance on redo generated from the production database has significant implications for operations in which Oracle E-Business Suite uses the nologging feature (described previously) to perform some resource-intensive tasks with faster throughput. Oracle recommends turning on the *force logging* feature at the database level to simplify your backup and recovery, and standby database maintenance procedures. In cases where the nologging feature is used in Release 12.2, and you have chosen not to use force logging, insufficient redo information will be generated to make the corresponding changes on the standby database. You may then be required to take manual steps to refresh the standby (or recreate the relevant objects) to ensure it will remain usable.

Finally, based on your organization's business requirements, choose one of the following protection modes:

- **Maximum protection**: This protection mode ensures that no data loss will occur if the primary database fails. To provide this level of protection, the redo data needed to recover each transaction must be written to both the local online redo log and to the standby redo log on at least one standby database before the transaction commits. To ensure data loss cannot occur, the primary database shuts down if a fault prevents it from writing its redo stream to the standby redo log of at least one transactionally-consistent standby database.
- **Maximum availability**: This protection mode provides the highest level of data protection that is possible without compromising the *availability* of the primary database. Like maximum protection mode, a transaction will not commit until the redo needed to recover that transaction is written to the local online redo log, and to the standby redo log of at least one transactionally-consistent standby database. However, unlike maximum protection mode, the primary database does not shut down if a fault prevents it from writing its redo stream to a remote standby redo log. Instead, the primary database switches to maximum performance mode until the fault is corrected, and all gaps in redo log files are resolved. When all gaps have been resolved, the primary database automatically resumes operating in maximum availability mode. This strategy ensures that no data loss will occur if the primary database fails, unless a second fault prevents a complete set of redo data from being sent from the primary database to at least one standby database.

- **Maximum performance**: This protection mode (the default) provides the highest level of data protection that is possible without affecting the *performance* of the primary database. This is accomplished by allowing a transaction to commit as soon as the redo data needed to recover that transaction is written to the local online redo log. The primary database's redo data stream is also written to at least one standby database, but that redo stream is written asynchronously with respect to the transactions that create the redo data. When network links with sufficient bandwidth are employed, this mode provides a level of data protection that approaches that of maximum availability mode, with minimal impact on primary database performance.

Flashback Database

Oracle recommends you enable the Flashback Database feature, to:

- Help protect against logical data corruption
- Allow you to reinstantiate the production database as a standby after a failover to your secondary site
- Create database restore points to which you can flash back in case an upgrade or major application change encounters a serious problem

Flashback Database enables you to rewind the database to a previous point in time without restoring backup copies of the data files. This is accomplished during normal operation by Flashback Database buffering and writing before images of data blocks into the *flashback logs*, which reside in the *flash recovery area*.

Flashback Database can also flashback a primary or standby database to a point in time prior to a Data Guard role transition. In addition, a Flashback Database operation can be performed to a point in time prior to a resetlogs operation, which allows administrators more flexibility to detect and correct human errors.

For further information, refer to My Oracle Support knowledge documents 1070491.1, *Using Active Data Guard Reporting with Oracle E-Business Suite Release 12.1 and Oracle Database 11g*, and 1070033.1, *Business Continuity for Oracle E-Business Release 12 Using Oracle 11g Physical Standby Database*.